REMARKS and ARGUMENTS

This is a Response to the Final Office Action mailed August 2, 2007 and is also in response to the Advisory Action mailed October 23, 2007.

Independent claims 90, 100, and 104 are currently amended.

Claims 93, 95, and 103 are canceled.

Claims 90–92, 94, 96–102, and 104–108 are pending.

Objections to Specification

Applicant's response dated October 2, 2007 addressed the Examiner's objections in the Office Action mailed August 2, 2007.

Claim Rejections – 35 USC § 112

Applicant's response dated October 2, 2007 addressed the Examiner's § 112 rejections in the Office Action mailed August 2, 2007.

Claim Rejections – 35 U.S.C. § 103

In the Office Action mailed August 2, 2007, independent claims 90, 100, and 104, and some claims dependent thereon, were rejected under 35 USC § 103(a) as being unpatentable over Ishibashi et al. (US 6,728,379 B1) hereinafter "Ishibashi" in view of McCarty (US 5,666,411) hereinafter "McCarty".

As stated in the recent Advisory Action with reference to limitation (e) in applicant's claim 90, "Ishibashi teaches encryption and decryption of information/data for transmission to another entity as shown in US 6728379 B1, Fig. 6, Steps 5 & 7.

"Thus when McCarty is combined with Ishibashi, the server would have to re-encrypt said unique identifier (contained in the upgrade data of McCarty). In other words, the combined invention of Ishibashi and McCarty teaches (e) reencrypting in said server [US 6728379 B1, Fig 6, Step 3] said chip identifier together with a decryption key [US 5666411, Col 10, Ln 61–66] corresponding to said first encryption key to produce an encrypted data block [encryption of DEVID/ Ed(SYSKEY) which comprise the upgrade data that would have been a result of the combined invention reading on the encryption data block.]."

Applicant has amended limitation (e) in claim 90 and other independent claims to add the words: "such that each bit in said encrypted data block is a complex function of every bit in said decryption key and every bit in said chip identifier".

Although encrypting said chip identifier (DEVID) and encrypting said decryption key (SYSKEY) in said server and transmitting them together in encrypted form to said cryptoprocessor would be obvious over the combined teachings of Ishibashi and McCarty, that is only a part of applicant's invention. In applicant's specification, as disclosed in paragraph 0049 with reference to Fig. 2, block encryption process 129 in server 120 "block encrypts [decryption] key K1 together with chip identifier 139 and random filler bits to produce key block 94." "It is important that these data fields be encrypted together as one block and not as individual fields or bytes, so that each bit in the encrypted block 94 is a complex function of every bit of the decrypted block [containing key K1, chip identifier 139, and filler bits] and of every bit of key K2".

The combined teachings of Ishibashi and McCarty does not show, describe, suggest, or teach this limitation in applicant's claim 90 (e). The phrases "each bit" or "every bit" do not appear in Ishibashi or McCarty. The proposed combination of Ishibashi and McCarty would not suggest that DEVID and SYSKEY be encrypted together in the same data block so that each bit of the encrypted data block will be a function of every bit of DEVID and every bit of SYSKEY. Nor is there any stated or implied motivation to do so.

Applicant's motivation is to prevent unauthorized persons from using an encrypted DEVID and encrypted SYSKEY separately and to prevent discovery of SYSKEY even if a DEVID becomes known. If DEVID and SYSKEY were encrypted separately, as in McCarty column 8 lines 14–18, unauthorized persons could use an encrypted un-authorized DEVID with an authorized encrypted SYSKEY and the security provided by combined use of DEVID with SYSKEY would be defeated.

Even if, for the sake of argument, the encryption of Ishibashi were applied to the DEVID and SYSKEY of McCarty to produce an encrypted data block containing both DEVID and SYSKEY in encrypted form, there is no suggestion in either Ishibashi or McCarty that each bit in the encrypted data block should be a complex function of every bit in DEVID and every bit in SYSKEY.

In summary, the proposed combination of Ishibashi and McCarty does not suggest or teach the following limitations in applicant's claims 90 or other pending claims: (e) reencrypting in said server said chip identifier together with a decryption key corresponding to said first encryption key to produce an encrypted data block such that each bit in said encrypted data block is a complex function of every bit in said decryption key and every bit in said chip identifier.

In order to establish a *prima facie* case of obviousness, all of the claim limitations must be taught or suggested by the prior art references when combined (MPEP 706.02(j)). All of the claim limitations in claims 90, 100, and 104 were not taught or suggested. Therefore no *prima facie* case of obviousness has been established.

In view of the above, each of the presently pending claims in this application is believed to be in condition for allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue.

Respectfully submitted,

GRAYBEAL JACKSON HALEY LLP

Jeffrey T. Haley
Registration No. 34,834
155 - 108th Avenue N.E., Suite 350
Bellevue, WA 98004-5901
(425) 455-5575.